ABSTRACT OF THE DISCLOSURE

A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network.